JOURNAL OF ALGEBRA **208,** 359–371 (1998)
ARTICLE NO. JA987517

Hilbert–Kunz Functions in a Family: Line-S_4 Quartics

Paul Monsky

Department of Mathematics, Brandeis University, Waltham, Massachusetts 02254-9110

Received December 1, 1997

INTRODUCTION

Let F be an algebraically closed field of characteristic 2. We shall complete the calculation, started in [1], of the Hilbert–Kunz functions of those quartics that admit a group of linear automorphisms isomorphic to S_4.

Recall the notation of [1]. $V = F^3$, $x, y, z \in \hat{V}$ are the coordinate functions on V and $S(\hat{V}) = F[x, y, z]$ is the algebra of polynomial functions on V. A subgroup G of $GL_3(F)$ acts on V and consequently on $\hat{V}$ and on $F[x, y, z]$. A quartic $g \in F[x, y, z]$ is a "G-quartic" if $g^\sigma = g$ for each σ in G, an S_4-quartic if it is a G-quartic for some G isomorphic to S_4, and nondegenerate if it has no linear factor. We showed that there are two conjugacy classes of S_4's in $GL_3(F)$; the "point-S_4's" and the "line-S_4's", and for each nondegenerate point-S_4 quartic g we calculated $e_n(g) = \dim F[x, y, z]/(g, x^{2^n}, y^{2^n}, z^{2^n})$ as well as $c(g) = \lim_{n\to\infty} e_n/4^n$. Explicitly we proved the following. If G is a point-S_4, the nondegenerate G-quartics are parametrized by $F - \{0\}$. To each α in the parameter set one attaches an $m = m(\alpha)$ which is either a positive integer or ∞; explicitly $m(\lambda^2 + \lambda)$ is the degree of λ over $Z/2$. Then $e_n(g_\alpha) = 3 \cdot 4^n - 4$ if $1 \le n \le m$ and $3 \cdot 4^n + 4^{n-m}$ if $n > m$, so that $c(g) = 3 + 4^{-m}$.

The results of this paper are in some ways similar. If G is a line-S_4 we show that the nondegenerate G-quartics h are parametrized by F. (More precisely let $A_x = x^2 + yz$ and $A_y = y^2 + xz$. Then for an appropriate G, each nondegenerate G-quartic is a constant multiple of $h_\alpha = \alpha z^4 + A_x A_y$ for some $\alpha \in F$.) To each α we attach an $l = l(\alpha)$ which is either a

0021-8693/98 $25.00

positive integer or ∞, and show that $e_n(h_\alpha) = 3 \cdot 4^n - 4$ if $1 \le n \le 2l$ and $3 \cdot 4^n + 4^{n-2l}$ if $n > 2l$, so that $c(h_\alpha) = 3 + 16^{-l}$. The big surprise is the definition of $l(\alpha)$—we construct a 1-parameter family of dynamical systems parametrized by F, and define $l(\alpha)$ to be an "escape time" for the system corresponding to α.

DEFINITION. (1) φ_α: $F \cup \{\infty\} \to F \cup \{\infty\}$ is the map $t \to t^4 + \alpha t^{-4}$. $\varphi_\alpha^{(1)} = \varphi_\alpha$ and $\varphi_\alpha^{(r+1)} = \varphi_\alpha \circ \varphi_\alpha^{(r)}$.

(2) The escape time, $l(\alpha)$, of α is r if $\varphi_\alpha^{(r)}(1) = 0$ and ∞ if no $\varphi_\alpha^{(r)}(1) = 0$.

[Note that if $\varphi_\alpha^{(r)}(1) = 0$ then $\varphi_\alpha^{(s)}(1) = \infty$ for $s > r$. So there is at most one r with $\varphi_\alpha^{(r)}(1) = 0$.]

Remark 1. If r is a positive integer we shall show that there are exactly 8^{r-1} values of α for which $l(\alpha) = r$. But these α appear to be quite irregularly distributed through F; see the examples at the end of the paper.

Remark 2. Note that $h_1 = z^4 + A_x A_y = x^2y^2 + P$ where $P = z^4 + xyz^2 + x^3z + y^3z$. In other words h_1 is just the g_1 of [1], and is both a point-S_4 quartic and a line-S_4 quartic. Indeed, h_1 is the characteristic 2 Klein quartic, stable under a group of linear automorphisms of $F[x, y, z]$ that is conjugate to $GL_3(Z/2)$, and $GL_3(Z/2)$ contains both point-S_4's and line-S_4's.

1. PRELIMINARIES

We describe a particular line-S_4. For $a \in GF(4)$ let $\nu_a = (a, a^2, 1)$. Then the ν_a sum to zero and span V. Let G consist of all endomorphisms of V which permute the ν_a. Evidently G is isomorphic to S_4. Then $\nu_a + \nu_b$ span a two-dimensional space, $z = 0$, stabilized by G, so G is a line-S_4. We easily find the following lemma.

LEMMA 1.1. *G is generated by the maps $(x, y, z) \to (x + az, y + a^2z, z)$, $a^4 = a$, together with the maps $(x, y, z) \to (y, x, z)$ and $(x, y, z) \to (ax, a^2y, z)$, $a^3 = 1$.*

Recall that a quartic is "nondegenerate" if it has no linear factor.

THEOREM 1.2. *Every G-quartic is a linear combination of z^4 and $A_x A_y$, where $A_x = x^2 + yz$, $A_y = y^2 + xz$. Consequently every nondegenerate G-quartic is a constant multiple of $h_\alpha = \alpha z^4 + A_x A_y$ for some α in F.*

Proof. Lemma 1.1 shows that z and A_xA_y are fixed by the elements of G. Suppose g is a G-quartic. Then each monomial appearing in g is fixed by $(x, y, z) \to (ax, a^2y, z)$ when $a^3 = 1$. Since g is also fixed by $(x, y, z) \to (y, x, z)$ it is a linear combination of z^4, A_xA_y, xyz^2, and x^2y^2. But one sees easily that no nontrivial linear combination of xyz^2 and x^2y^2 is fixed by the map $(x, y, z) \to (x + z, y + z, z)$. The last assertion follows immediately. ∎

In [1] we made use of identities involving powers of P. Here we shall need identities involving powers of A_x and A_y. Suppose that $q \geq 4$.

DEFINITION 1.3. (a) $S_x(q) = \sum A_y^{q_0} z^{q-2q_0} + \sum A_x^{q_0} z^{q-2q_0}$ where the first (resp. second) sum runs over all q_0 dividing $q/4$ with q/q_0 a square (resp. nonsquare).

(b) $R_x(q) = xz^{q-1}$ or yz^{q-1} according as q is a square or not.

(c) $S_y(q)$ and $R_y(q)$ are the images of $S_x(q)$ and $R_x(q)$ under the map $x \to y$, $y \to x$.

LEMMA 1.4. *If q is a square (resp. nonsquare) then both $S_x(2q) + S_x(q)^2$ and $R_x(2q) + R_x(q)^2$ are A_xz^{2q-2} (resp. A_yz^{2q-2}).*

Proof. Suppose q is a square. The term in $S_x(2q)$ corresponding to $q_0 = 1$ is A_xz^{2q-2}. Also the term in $S_x(q)^2$ corresponding to q_0 is equal to the term in $S_x(2q)$ corresponding to $2q_0$, and we get the first equality. Furthermore $R_x(2q) + R_x(q)^2 = yz^{2q-1} + x^2z^{2q-2} = A_xz^{2q-2}$. The argument when q is a nonsquare is similar. ∎

THEOREM 1.5. $A_x^{q/2} + x^q = S_x(q) + R_x(q)$, $A_y^{q/2} + y^q = S_y(q) + R_y(q)$.

Proof. When $q = 4$ this is clear. By Lemma 1.4, $S_x(2q) + R_x(2q) = (S_x(q) + R_x(q))^2$ and the first result follows by induction. Applying the map $x \to y$, $y \to x$ we get the second result. ∎

DEFINITION 1.6. Fix $q \geq 4$. Then $O = F[x, y, z]/(x^q, y^q, z^q)$, and S_x, S_y, R_x, R_y are the images of $S_x(q)$, $S_y(q)$, $R_x(q)$, $R_y(q)$ in O.

COROLLARY 1.7. *In the ring O, $A_x^{q/2} = S_x + R_x$ and $A_y^{q/2} = S_y + R_y$. Furthermore z annihilates R_x and R_y.*

DEFINITION 1.8. H is the order 8 subgroup of G consisting of the maps $(x, y, z) \to (x + az, y + a^2z, z)$ and $(x, y, z) \to (y + az, x + a^2z, z)$ with $a^4 = a$. O^H is the fixed subring of O under the action of H. (Note that O^H contains h_α as well as z, A_xA_y and all the $A_x^iA_y^j + A_x^jA_y^i$.) N (resp. N^H) is the homogeneous ideal of O (resp. O^H) consisting of elements annihilated by h_α.

We now indicate our strategy for calculating $e_n(h)$ where $h = h_\alpha$. In Section 2 we define some simple linear maps and express their nullities in terms of escape times, using an inductive argument that is based on elementary row and column transformations. These results and calculations in O^H combine in Section 3 to give the dimension of $N^H_{(3q/2)-4}$, and in particular to show that this dimension is 0 when $q < 2 \cdot 4^{l(\alpha)}$ and 1 when $q = 2 \cdot 4^{l(\alpha)}$. A similar calculation in Section 4 shows that $N_{(3q/2)-5} \neq (0)$ when $q = 2 \cdot 4^{l(\alpha)}$. The estimates from Sections 3 and 4, when combined with techniques from [1], give the e_n.

2. NULLITIES AND ESCAPE TIMES

It is convenient to generalize the notion of escape time. Fix $\alpha \in F$ and let $X = 2^Z \times (F \cup \{\infty\})$, where 2^Z is the subgroup of Q^* generated by 2.

DEFINITION 2.1. Φ_α: $X \to X$ is the map $(q, t) \to (q/4, t + \alpha^q t^{-1})$. (Since F is algebraically closed, α^q makes sense even if $q < 1$.)

DEFINITION 2.2. $\Phi_\alpha^{(0)}$ is the identity map and $\Phi_\alpha^{(r+1)} = \Phi_\alpha \circ \Phi_\alpha^{(r)}$. Suppose $x = (q, t)$ is in X with $t \neq \infty$. If $\Phi_\alpha^{(r)}(x) = (q/4^r, 0)$ we say that $l_\alpha(x) = r$. If no $\Phi_\alpha^{(r)}(x)$ is $(q/4^r, 0)$ we say that $l_\alpha(x) = \infty$.

Remark. The above definition is ambiguous only when $\alpha = 0$, $t = 0$ and $x = (q, 0)$, in which case $\Phi_\alpha^{(r)}(x) = (q/4^r, 0)$ for all r. But this case will not concern us.

LEMMA 2.3. *For all q in 2^Z, $l_\alpha(q, 1) = l_\alpha$.*

Proof. Evidently $\Phi_\alpha(q, t^{4q}) = (q/4, (\varphi_\alpha(t))^q)$. It follows that $\Phi_\alpha^{(r)}(q, t^{4q}) = (q/4^r, (\varphi_\alpha^{(r)}(t))^{4q/4^r})$. Setting $t = 1$ gives the result. ∎

We next define some simple linear maps, and show that their nullities are related to the $l_\alpha(q, t)$.

DEFINITION 2.4. Suppose α and t are in F and $q \geq 1$ is a power of 2. Let U and U' be vector spaces over F with bases $\{u_i\}$ and $\{v_i\}$, $1 \leq i \leq q - 1$. Let T: $U \to U'$ be the linear map with $T(u_i) = \alpha^{q-i} v_i + t \sum v_j$ where the sum ranges over all indices j such that $i + j = q/4^s$, for some $s \geq 0$. Then $N_\alpha(q, t)$ is the nullity of T.

Remark. For applications to Hilbert–Kunz functions we only need to know the $N_\alpha(q, 1)$. But our inductive procedure necessitates the study of all the $N_\alpha(q, t)$.

LEMMA 2.5. *Let q be a power of 2 and $v_1, \ldots, v_{q-1}$ be elements of a vector space over F. Suppose that, for $1 \leq j \leq q - 1$, $F_j = \sum v_i$, the sum*

extending over all indices i with $i + (q - j) = q/4^s$ for some s. Then the same formula holds if the v's and F's are interchanged. In particular $v_{q-i} = \Sigma F_j$, the sum extending over all j with $i + j = q/4^s$ for some s.

Proof. Let M be the matrix expressing the F's as linear combinations of the v's. Then $m_{i,i} = 1$, and if $i \neq j$, $m_{i,j} = 0$ unless $j \geq i + q - q/4$. So $(M - I)^2 = 0$ and $M^2 = I$. ∎

LEMMA 2.6. *Notation as in Definition* 2.4. *Then the following linear maps $U \to U'$ have the same nullity*:

(a) $u_i \to tv_i + \alpha^i \Sigma v_j$,

(b) $u_i \to \alpha^{q-i} v_i + t\Sigma v_j$,

where in each case the sum extends over all indices j with $i + j = q/4^s$ for some $s \geq 0$.

Proof. Let $E_i = u_{q-i}$. Then under (a), $E_i \to \alpha^{q-i}\Sigma v_j + tv_{q-i}$ where the sum extends over all j with $j + (q - i) = q/4^s$ for some s. If we define the F_j as in Lemma 2.5, and use Lemma 2.5 we find that under (a), $E_i \to \alpha^{q-i}F_i + t\Sigma F_j$, the sum extending over all j with $i + j = q/4^s$ for some s. The lemma follows. ∎

LEMMA 2.7. *Suppose $q \geq 4$ and $t \neq 0$. Let $t^* = t + \alpha^q t^{-1}$. Then*

(1) *If $t^* \neq 0$, $N_\alpha(q, t) = N_\alpha(q/4, t^*)$.*

(2) *If $t^* = 0$, $N_\alpha(q, t) = (q/4) + 1$.*

Proof. For each $i < q/2$ let $E_i = \alpha^i t^{-1} u_i + u_{q-i}$ and $F_i = v_i$. If $i < q/2$, $T(u_i) = \alpha^{q-i}F_i + tv_{q-i} + t\Sigma F_j$, the sum extending over all j with $i + j = q/4^s$ for some s. Furthermore $T(u_{q-i}) = \alpha^{q-i} v_{q-i} + tF_i$. It follows that $T(E_i) = t^*F_i + \alpha^i \Sigma F_j$, with the sum as before. So we get the following formulas:

(1) $T(E_i) = t^*F_i + \alpha^i \Sigma F_j$, $i \leq (q/4) - 1$.

(2) $T(E_i) = t^*F_i$, $q/4 \leq i < q/2$.

(3) $T(u_{q/2}) = (\alpha^{q/2} + t)v_{q/2}$.

(4) $T(u_i) = \alpha^{q-i} v_i + tF_{q-i}$, $q/2 < i < q$.

When $\alpha = 0$, $t^* = t$, and we see easily that $N_\alpha(q, t) = N_\alpha(q/4, t) = 0$. Suppose $\alpha \neq 0$. Then the E_i, together with the u_i, $(q/2 < i < q)$, form a basis of U. If $t^* \neq 0$, $\alpha^{q/2} + t \neq 0$ and we conclude that the kernel of T is contained in the subspace spanned by the E_i with $i \leq (q/4) - 1$. Formula (1) combined with Lemma 2.6 shows that this nullity is $N^\alpha(q/4, t^*)$. Suppose that $t^* = 0$. Then T annihilates the E_i with $q/4 \leq i < q/2$ as well as $u_{q/2}$, and the nullity is $(q/4) + 1$. ∎

THEOREM 2.8. *Suppose* $t \neq 0$; *let* $l = l_\alpha(q,t)$. *Then if* $q < 4^l/2$, $N_\alpha(q,t) = 0$.

Proof. We argue by induction on q, $q = 1$ being trivial. Suppose $q \geq 2$. Then $l > 1$ and consequently $t^* = t + \alpha^q t^{-1} \neq 0$. If $q = 2$ this tells us that $t \neq \alpha$, that $T(u_1) = (t + \alpha)v_1 \neq 0$ and that $T\colon U \to U'$ is $1 - 1$. If $q \geq 4$, $\Phi_\alpha(q,t) = (q/4, t^*)$. So if we set $l^* = l_\alpha(q/4, t^*)$, $l^* = l - 1$, $q/4 < 4^{l^*}/2$, and by induction $N_\alpha(q/4, t^*) = 0$. Now apply Lemma 2.7. ∎

THEOREM 2.9. *Suppose* $t \neq 0$ *and that* $l = l_\alpha(q,t) < \infty$. *Then if* $q = 4^l/2$, $N_\alpha(q,t) = 1$, *while if* $q \geq 4^l$, $N_\alpha(q,t) = (q/4^l) + 1$.

Proof. Suppose $l = 1$, so that $t^* = t + \alpha^q t^{-1} = 0$. When $q = 2$, $t = \alpha$ and $T\colon U \to U'$ is the zero map. When $q \geq 4$ we apply Lemma 2.7. Suppose now that $l > 1$, so that $q \geq 4$ and $t^* \neq 0$. Define l^* as in the proof of Theorem 2.8. When $q = 4^l/2$, $q/4 = 4^{l^*}/2$, induction tells us that $N_\alpha(q/4, t^*) = 1$ and we apply Lemma 2.7. When $q > 4^l/2$, $q/4 > 4^{l^*}/2$, induction tells us that $N_\alpha(q/4, t^*) = (q/4^l) + 1$ and again Lemma 2.7 gives the result. ∎

Combining Theorems 2.8 and 2.9 with Lemma 2.3 we find the following theorem.

THEOREM 2.10. *Let* $\alpha \in F$ *and* $l = l(\alpha)$. *Then* $N_\alpha(q,1) = 0$ *if* $q < 4^l/2$, 1 *if* $q = 4^l/2$ *and* $(q/4^l) + 1$ *if* $q \geq 4^l$.

A variation on Theorem 2.10 will be useful. Let U_1 be the subspace of U spanned by the u_i with i odd, and U_1' the subspace of U' spanned by the v_i with i odd. Evidently the T of Definition 2.4 restricts to a map $T^-\colon U_1 \to U_1'$.

DEFINITION 2.11. $N_\alpha^-(q,t)$ is the nullity of T^-.

THEOREM 2.12. *Suppose* $t \neq 0$ *and that* $l = l_\alpha(q,t) < \infty$. *Then if* $q = 4^l/2$, $N_\alpha^-(q,t) = 1$.

Sketch of proof. When $l = 1$, $q = 2$, $T = T^-$ and we apply Theorem 2.9. For $l > 1$ we proceed by induction as in the proof of Theorem 2.9, the critical step being to show that $N_\alpha^-(q,t) = N_\alpha^-(q/4, t^*)$. But the arguments of Lemma 2.5, 2.6, and 2.7 go through unchanged to prove this equality. Taking $t = 1$ we get the following corollary.

COROLLARY 2.13. *Let* $\alpha \in F$ *and* $l = l(\alpha)$. *If* $l < \infty$, $N_\alpha^-(4^l/2, 1) = 1$.

3. $N^H_{(3q/2)-4}$

Throughout α is a fixed element of F, $h = h_\alpha$, $q \geq 4$, and H, O, O^H, N, and N^H are as in Definition 1.8. Our goal is to show that dim $N^H_{(3q/2)-4} = N_\alpha(q/4, 1)$. Together with Theorem 2.10 this will give Theorem 3.1.

THEOREM 3.1. *Let* $l = l(\alpha)$. *Then* dim $N^H_{(3q/2)-4} = 0$ *if* $q \leq 4^l$, 1 *if* $q = 2 \cdot 4^l$ *and* $(q/4^{l+1}) + 1$ *if* $q \geq 4^{l+1}$.

DEFINITION 3.2. $[i, i] = A^i_x A^i_y$. If $i \neq j$, $[i, j] = A^i_x A^j_y + A^j_x A^i_y$.

DEFINITION 3.3. V^* is the subspace of $O^H_{(3q/2)-4}$ spanned by the $[i, j]z^k$ with $i \leq j < q/2$, $k < q$ and $2i + 2j + k = (3q/2) - 4$. $V \subset V^*$ is spanned by these elements excluding $[(q/4) - 1, (q/2) - 1]$.

DEFINITION 3.4. $V_0 \subset V$ is spanned by all the above elements for which $j \neq (q/2) - 1$.

DEFINITION 3.5. V' is the subspace of $O^H_{(3q/2)}$ spanned by the $[i, j]z^k$ with $i \leq j < q/2$, $k < q$ and $2i + 2j + k = 3q/2$. $(V')^*$ is spanned by V' together with $A^{q/4}_x R_y + A^{q/4}_y R_x$.

THEOREM 3.6. $h \cdot V \subset V'$, $h \cdot V^* \subset (V')^*$ *and the induced map* $V^*/V \to (V')^*/V'$ *is onto*.

Proof. $z^4 V \subset V'$. So to show that $h \cdot V \subset V'$ it is enough to show that $[i + 1, j + 1]z^4$ is in V' when $[i, j]z^k$ is one of the generators of V given in Definition 3.3. If $j \neq (q/2) - 1$ this is clear. If $j = (q/2) - 1$ we must have $0 \leq i \leq (q/4) - 2$ and $k \neq 0$. Then $[i + 1, j + 1]z^k = (A^{i+1}_x A^{q/2}_y + A^{q/2}_x A^{i+1}_y)z^k$. By Corollary 1.7 this is $(A^{i+1}_x S_y + A^{i+1}_y S_x)z^k + (A^{i+1}_x R_y + A^{i+1}_y R_x)z^k$; the first term is evidently in V' and the second is 0 since $k \geq 1$ and $zR_x = zR_y = 0$. The same argument shows that $h[(q/4) - 1, (q/2) - 1] =$ (an element of V') $+ A^{q/4}_x R_y + A^{q/4}_y R_x$, completing the proof. ∎

DEFINITION 3.7. Let $u \neq 0$ be in O_k for some k. Then u is a linear combination of degree k monomials, each having degree $< q$ in each of x, y, and z and we may expand u in *ascending* powers of z: $u = A(x, y)z^r + \cdots$. The "minimal z-degree" of u is r, and the "lowest term" of u is $A(x, y)z^r$.

Remarks. This contrasts with [1] where u was expanded in descending powers of z. But once again we find that if $u_i \in O_k$ have linearly independent lowest terms then the u_i themselves are linearly independent. Note also that if $i \leq j < q/2$ and $k < q$ then the lowest term of $[i, j]z^k$ is $x^{2i}y^{2i}z^k$ if $i = j$ and $(x^{2i}y^{2j} + x^{2j}y^{2i})z^k$ otherwise. Furthermore $A^{q/4}_x R_y + A^{q/4}_y R_x = (x^{q/2}y + y^{q/2}x)z^{q-1}$ or $(x^{(q/2)+1} + y^{(q/2)+1})z^{q-1}$ according as q a square or nonsquare. One consequence is that the generators of V^*

[resp. $(V')^*$] given in Definition 3.3 (resp. 3.5) are a basis. Another is that any element of $(V')^*$ of minimal z-degree $q-1$ is a constant multiple of $A_x^{q/4}R_y + A_y^{q/4}R_x$, and so cannot be divisible by x^2y^2.

LEMMA 3.8. *Suppose $u \in O^H$ is homogeneous of minimal z-degree $r < q-1$. Then the lowest term of u is Az^r where A is a polynomial in x^2 and y^2.*

Proof. Write $u = A(x,y)z^r + B(x,y)z^{r+1} + \cdots$. Suppose $a^3 = 1$. Since u is fixed by $\sigma\colon x \to x + az$, $y \to y + a^2z$, and $r+1 < q$, a comparison of the coefficients of z^{r+1} in u and u^σ shows that $a(\partial A/\partial x) + a^2(\partial A/\partial y) = 0$. Since this is true for all a with $a^3 = 1$, $\partial A/\partial x = \partial A/\partial y = 0$. ∎

THEOREM 3.9. $N^H_{(3q/2)-4} \subset V$.

Proof. Since V^*/V and $(V')^*/V'$ are one-dimensional, Theorem 3.6 shows that multiplication by h maps V^*/V 1-1 to $(V')^*/V'$. So any element of V^* annihilated by h is in V, and it suffices to show that $N^H_{(3q/2)-4} \subset V^*$. We shall show that if $u \in O^H_{(3q/2)-4}$ and $hu \in (V')^*$ then $U \in V^*$, arguing by descending induction on the minimal z-degree, r, of u. If $r = q-1$, $u = A(x,y)z^{q-1}$ with $\deg A = (q/2) - 3$. Then $x^2y^2A \neq 0$, and $hu = x^2y^2Az^{q-1}$ is an element of $(V')^*$ of minimal z-degree $q-1$, divisible by x^2y^2, contradicting the remarks after Definition 3.7. Suppose $r < q-1$. Using Lemma 3.8 and the fact that u is invariant under $x \to y$, $y \to x$ we find that the lowest term in u is a linear combination of $x^{2i}y^{2i}z^r$ and $(x^{2i}y^{2j} + x^{2j}y^{2i})z^r$. Taking v to be an appropriate linear combination of $[i,i]z^r$ and $[i,j]z^r$ we find that $u - v$ has minimal z-degree $> r$. Since $v \in V^*$, $h(u-v)$, like hu, is in $(V')^*$. By induction $u - v \in V^*$, and so is u. ∎

THEOREM 3.10. *The map $V/V_0 \to V'/hV_0$ induced by multiplication by h has kernel isomorphic to $N^H_{(3q/2)-4}$.*

Proof. Since $N^H_{(3q/2)-4} \subset V$, the kernel identifies with $(N_{(3q/2)-4} + V_0)/V_0$, and it suffices to show that $V_0 \cap N = (0)$. Suppose then that $u \neq 0$ is in V_0. Then the lowest term of u is a linear combination of $x^{2i}y^{2i}z^r$ and $(x^{2i}y^{2j} + x^{2j}y^{2i})z^r$ with $i < j \leq (q/2) - 2$. Thus x^2y^2 annihilates no monomial appearing in this lowest term, and $hu \neq 0$. ∎

DEFINITION 3.11. Suppose $1 \leq i < q/4$. Define $u_i \in V$ and $v_i \in V'$ by

$$u_i = [(q/4) - i - 1, (q/2) - 1]z^{2i},$$
$$v_i = [0, (q/4) + i]z^{q-2i}.$$

THEOREM 3.12. *The u_i are a basis of V/V_0 and the v_i are a basis of V'/hV_0.*

Proof. The u's are just those elements $[i, j]z^k$ of the basis of V given in Definition 3.3 for which $j = (q/2) - 1$. Since the remaining elements of the basis generate V_0 we get the first result. Now let t_r be the basis of V_0 given in Definition 3.4. Then the $A_x A_y t_r$ and the v_i are the basis of V' given in Definition 3.5. Now the ht_r and the v_i also lie in V', and have exactly the same lowest terms as the $A_x A_y t_r$ and the v_i. It follows that they also form a basis of V', completing the proof. ∎

LEMMA 3.13. *Suppose that* $i \le j < q/2$ *and that* $2i + 2j + k = 3q/2$. *Then*

$$[i, j] \cdot z^k \in hV_0 \text{ if } j - i \le q/4,$$
$$[i, j] \cdot z^k \equiv \alpha^i v_{j-i-(q/4)}(hV_0) \text{ if } j - i > q/4.$$

Proof. We argue by induction on i. Suppose first that $i = 0$. Then if $j \le q/4$, $k \ge q$, and $[i, j] \cdot z^k = 0$ in O. And if $j > q/4$, then $[i, j]z^k = [0, j]z^{(3q/2)-2j} = v_{j-(q/4)}$. Suppose $i > 0$. Then $w = [i - 1, j - 1]z^k$ is in V_0, and $hw = [i, j]z^k + \alpha[i - 1, j - 1]z^{k+4}$. By induction $[i - 1, j - 1]z^{k+4} \equiv \alpha^{i-1} v_{j-i-(q/4)}$, giving the lemma. ∎

THEOREM 3.14. *Let* T *be the map of Theorem* 3.10. *Then* $T(u_i) = \alpha^{(q/4)-i} v_i + \sum v_j$ *where the sum ranges over all indices* j *such that* $i + j = (q/4^s)$ *for some* $s \ge 1$. *In particular, the nullity of* T *is* $N_\alpha(q/4, 1)$.

Proof. $T(u_i) = \alpha[(q/4) - i - 1, (q/2) - 1]z^{2i+4} + [(q/4) - i, q/2]z^{2i}$. By Lemma 3.13 the first term is $\alpha \cdot \alpha^{(q/4)-i-1} \cdot v_i$. By Corollary 1.7 the second term is $(A_x^{(q/4)-i} S_y + A_y^{(q/4)-i} S_x)z^{2i}$.

Expanding S_x and S_y as in Definition 1.3 we get a sum of terms of two types. Those of the first type are $[0, (q/4) - i + q_0]z^{q+2i-2q_0}$ where q_0 divides $q/4$ and q/q_0 is a square. But this is just v_{q_0-i}, and $q_0 = q/4^s$ for some $s \ge 1$. The terms of the second type are $[(q/4) - i, q_0]z^{q+2i-2q_0}$ where q_0 divides $q/4$ and q/q_0 is a nonsquare. Lemma 3.13 shows that all such terms are in hV_0, and the theorem follows. ∎

Combining Theorems 3.14 and 3.10 we find that $\dim N^H_{(3q/2)-4} = N_\alpha(q/4, 1)$, and Theorem 3.1 follows.

COROLLARY 3.15. *If* $1 \le n \le 2l(\alpha)$ *then* $e_n(h_\alpha) = 3 \cdot 4^n - 4$. *In particular if* $l(\alpha) = \infty$, *then* $c(h_\alpha) = 3$.

Proof. When $n = 1$ this is easy. Suppose $n \ge 2$ and set $q = 2^n$. Then $q \le 4^l$ and $N^H_{(3q/2)-4} = (0)$. Since H is a 2-group, Lemma 4.10 of [1] shows that $N_{(3q/2)-4} = (0)$. Corollary 4.2 of [1] then gives the result. ∎

4. $N^H_{(3q/2)-5}$

Fix α with $l = l(\alpha) < \infty$ and set $q = 2 \cdot 4^l$. Theorem 3.1 shows that $N^H_{(3q/2)-4}$ has dimension 1. In this section we show that $N^H_{(3q/2)-5}$ is nontrivial. The argument is similar to that of the last section and we leave some details to the reader. The case $l = 1$ can be settled by an easy calculation. For when $l = 1$, $\alpha = 1$ and $q = 8$, and the element $[0, 3] \cdot z$ of O^H_7 is easily seen to be annihilated by $z^4 + A_x A_y$. So from now on we assume $l \geq 2$, so that $q \geq 32$.

DEFINITION 4.1. W is the subspace of $O^H_{(3q/2)-5}$ spanned by the $[i, j]z^k$ with $i < j < q/2$, $k < q$, $k \equiv 1(4)$, and $2i + 2j + k = (3q/2) - 5$, together with $[0, (q/4) - 2]z^{q-1}$.

DEFINITION 4.2. $W_0 \subset W$ is spanned by all the $[i, j]z^k$ of Definition 4.1 with $j \neq (q/2) - 1$, together with $[0, (q/4) - 2]z^{q-1}$.

DEFINITION 4.3. W' is the subspace of $O^H_{(3q/2)-1}$ spanned by the $[i, j]z^k$ with $i < j < q/2$, $k < q$, $k \equiv 1(4)$, and $2i + 2j + k = (3q/2) - 1$, together with $[1, (q/4) - 1]z^{q-1}$.

THEOREM 4.4. $h_\alpha \cdot W \subset W'$.

Proof. The only essential respect in which the proof differs from that of Theorem 3.6 is in showing that $A_x A_y \cdot [(q/4) - 1, (q/2) - 1]z$ is in W'. Arguing as in the proof of Theorem 3.6 we see that this element is $(A_x^{(q/4)-1} S_y + A_y^{(q/4)-1} S_x)z$. We write S_x and S_y as sums of terms, one for each q_0 dividing $q/4$. The contribution that a $q_0 > 1$ makes to $(A_x^{(q/4)-1} S_y + A_y^{(q/4)-1} S_x)z$ is of the form $[i, j]z^k$ where $k = q + 1 - 2q_0$ is $\equiv 1(4)$, while the contribution from $q_0 = 1$ is $[1, (q/4) - 1]z^{q-1}$. (Here we use the fact that $q > 8$.) ∎

DEFINITION 4.5. Suppose i is odd and $1 \leq i < q/4$. Define $u_i \in W$ and $v_i \in W'$ by

$$u_i = [(q/4) - i - 1, (q/2) - 1]z^{2i-1},$$
$$v_i = [0, (q/4) + i]z^{q-2i-1}.$$

THEOREM 4.6. *The u_i represent a basis of W/W_0 and the v_i represent a basis of W'/hW_0.*

THEOREM 4.7. *Suppose that i is odd, $1 \leq i < q/4$. Then, in W'/hW_0, $hu_i = \alpha^{(q/4)-i} v_i + \Sigma v_j$, the sum extending over all odd j such that $i + j = q/4^s$ for some $s \geq 1$. Consequently the dimension of the kernel of the map $W/W_0 \to W'/hW_0$ induced by multiplication by h is $N^-_\alpha(q/4, 1)$.*

THEOREM 4.8. *There is a nonzero element of W annihilated by h. So $N^H_{(3q/2)-5} \neq 0$.*

Proof. Theorem 4.7 and Corollary 2.13 show that the multiplication by h map $W/W_0 \to W'/hW_0$ has nontrivial kernel; the result follows immediately. ∎

5. CALCULATION OF e_n

Suppose that $l = l(\alpha) < \infty$. Set $h = h_\alpha$. At the end of Section 3 we showed that $e_n(h) = 3 \cdot 4^n - 4$ for $1 \leq n \leq 2l$. We shall now prove that $e_n = 3 \cdot 4^n + 4^{n-2l}$ for $n > 2l$. One direction is easy.

THEOREM 5.1. *If $n > 2l$, $e_n \geq 3 \cdot 4^n + 4^{n-2l}$.*

Proof. According to Lemma 4.4 of [1], $e_{n+1} \geq 4e_n$ for all n. So it suffices to show that $e_{2l+1} \geq 3 \cdot 4^{2l+1} + 4$. Let $q = 2 \cdot 4^l$. By Theorem 4.8, $\dim N_{(3q/2)-5} \geq 1$. We can then proceed as in the proof of Lemma 4.6 of [1], showing first that $\dim N_{(3q/2)-4} \geq 3$, and then that

$$e_{2l+1} \geq (3 \cdot 4^{2l+1} - 4) + 2\big(\dim N_{(3q/2)-5} + \dim N_{(3q/2)-4}\big) \geq 3 \cdot 4^{2l+1} + 4.$$

∎

Suppose now that $q = 2^{2l+r}$ with $r \geq 1$.

LEMMA 5.2. $N^H_{(3q/2)-4-2^{r-1}} \neq (0)$.

Proof. $r = 1$ is Theorem 4.8. For $r > 1$ we argue by induction. Let $O^{(1)} = F[x, y, z]/(x^{q/2}, y^{q/2}, z^{q/2})$. By induction there is a $u \neq 0$ in $O^{(1)}_{(3q/4)-4-2^{r-2}}$ that is annihilated by h and fixed by H. Then u^2 may be viewed as a nonzero element of $O^H_{(3q/2)-8-2^{r-1}}$ annihilated by h^2. If $hu^2 \neq 0$ we are done. If $hu^2 = 0$, then $z^4u^2 \in N^H_{(3q/2)-4-2^{r-1}}$ and is nonzero by Lemma 4.5 of [1]. ∎

LEMMA 5.3. *Choose $u \neq 0$ in $N_{(3q/2)-4-2^{r-1}}$. Then for $s \leq 2^{r-2} + 1$ the $(A_x + A_y)^i z^{2j} u$ with $i + j = s$ are linearly independent.*

Proof. $A_x + A_y = (x + y)^2 + (x + y) \cdot z$. If follows that any linear combination of $A_x + A_y$ and z^2 is a product of two linear factors. Now, if the lemma were false, u would be annihilated by a form of degree s in $A_x + A_y$ and z^2, and consequently by a product of $2s$ linear forms. One would then get a nonzero element of N of degree $\leq (3q/2) - 3$ annihilated by a linear form, contradicting Lemma 4.5 of [1]. ∎

LEMMA 5.4. *Suppose* $q = 2^{2l+r}$ *with* $r \geq 2$; *choose* u *as in Lemma* 5.3. *Then for each* $s \leq 2^{r-2}$ *the* $(A_x + A_y)^i z^{2j} u$ *with* $i + j = s$ *are a basis of* $N^H_{(3q/2)+2s-4-2^{r-1}}$. *Furthermore when* $i = (\deg u) - 2$, $N^H_i = (0)$.

Proof. We argue by descending induction on s. When $s = 2^{r-2}$, Theorem 3.1 tells us that $\dim N^H_{(3q/2)-4} = (q/4^{l+1}) + 1 = s + 1$, and Lemma 5.3 gives the result. Suppose $s < 2^{r-2}$. It suffices to show that the $(A_x + A_y)^i z^{2j} u$ with $i + j = s$ span. So suppose $v \in N^H_{(3q/2)+2s-4-2^{r-1}}$. By induction $v_1 = (A_x + A_y)v$ and $v_2 = z^2 v$ are linear combinations of $(A_x + A_y)^i z^{2j} u$ with $i + j = s + 1$. Furthermore $z^2 v_1 = (A_x + A_y)v_2$. Since $s + 2 \leq 2^{r-2} + 1$, the $(A_x + A_y)^i z^{2j} u$ with $i + j = s + 2$ are linearly independent, and it follows that there is a linear combination w of the $(A_x + A_y)^i z^{2j} u$, $i + j = s + 1$, such that $v_1 = (A_x + A_y)w$ and $v_2 = z^2 w$. Then z^2 annihilates $v - w$, and Lemma 4.5 of [1] shows that $v = w$. Suppose finally that $v \in N^H_i$ with $i + 2 = \deg u$. By what we have proved, $(A_x + A_y) \cdot v = b_1 u$ and $z^2 v = b_2 u$. So $b_1 z^2 + b_2(A_x + A_y)$ annihilates u. By Lemma 5.3, $b_1 = b_2 = 0$, and Lemma 4.5 of [1] shows that $v = 0$. ∎

LEMMA 5.5. *Suppose* $q = 2^{2l+r}$ *with* $r \geq 2$ *and* $0 \leq s \leq 2^{r-1} + 3$. *Then the dimension of* $N_{(3q/2)+s-7-2^{r-1}}$ *is* $\leq 4s - 4$ *if* s *is odd and* $\leq 4s$ *if* s *is even*.

Proof. Suppose first that s is odd. Then Lemma 5.4 shows that $\dim N^H_{(3q/2)+s-7-2^{r-1}} = (s - 1)/2$. Since $|H| = 8$ the result follows from Lemma 4.10 of [1]. If s is even we use the result for $s + 1$ together with the fact that multiplication by z is $1 - 1$ on $N_{(3q/2)+s-7-2^{r-1}}$. ∎

LEMMA 5.6. *Suppose* $q = 2^{2l+r}$ *with* $r \geq 2$. *Then* $\dim O/hO \leq (3q^2 - 4) + (2^r + 6)(2^r + 8)$.

Proof. Lemma 5.5 together with Lemma 4.1 of [1] shows that $\dim O/hO \leq (3q^2 - 4) + 2\sum_1^{2^{r-1}+3}(4i)$. ∎

THEOREM 5.7. $c(h) = 3 + 16^{-l}$ *where* $l = l(\alpha)$.

Proof. If $r \geq 2$, Lemma 5.6 shows that $e_{2l+r}(h) \leq 3 \cdot 4^{2l+r} + (2^r + 6)(2^r + 8)$. Dividing by 4^{2l+r} and letting $r \to \infty$ we find that $c(h) \leq 3 + 16^{-l}$. The opposite inequality comes from Theorem 5.1. ∎

THEOREM 5.8. *If* $n > 2l$, $e_n(h) = 3 \cdot 4^n + 4^{n-2l}$.

Proof. We have already seen that $e_n(h) \geq 3 \cdot 4^n + 4^{n-2l}$. Suppose that strict inequality holds for some n. Since $e_{n+1} \geq 4e_n$ for all n it would follow that $c(h) > 3 + 16^{-l}$, contradicting Theorem 5.7. ∎

We conclude the paper by showing that for each positive integer l there are exactly 8^{l-1} parameter values α for which $l(\alpha) = l$, and consequently exactly $8^{l-1} h_\alpha$ with $c(h_\alpha) = 3 + 16^{-l}$.

DEFINITION 5.9. G_n and $H_n \in F$ are defined by

(1) $G_1 = \alpha + 1$ and $H_1 = 1$.

(2) $G_{n+1} = G_n^8 + \alpha H_n^8$, $H_{n+1} = G_n^4 H_n^4$.

THEOREM 5.10.

(1) *G_n and H_n cannot both be zero for any n.*

(2) *G_n, viewed as a polynomial in α, has 8^{n-1} distinct roots in F.*

(3) *$l(\alpha) = n$ if and only if $G_n(\alpha) = 0$.*

Proof. When $\alpha = 0$ all the G_n and H_n are 1. Suppose $\alpha \neq 0$ and $G_{n+1} = H_{n+1} = 0$. Since $H_{n+1} = G_n^4 H_n^4$, either G_n or H_n is 0. Since $G_{n+1} = G_n^8 + \alpha H_n^8$, $G_n = H_n = 0$. Continuing we find that $G_1 = H_1 = 0$. This contradiction establishes (1). Now view G_n and H_n as polynomials in α. An easy induction shows that $\deg G_n = 8^{n-1}$ and $\deg H_n < 8^{n-1}$. Also $G'_{n+1} = H_n^8$. So if α is a multiple root of G_{n+1}, $H_n = 0$ and $G_{n+1} = H_{n+1} = 0$ contradicting (1). Finally $\varphi_\alpha(1) = 1 + \alpha = G_1/H_1$, while $\varphi_\alpha(G_n/H_n) = (G_n^8 + \alpha H_n^8)/G_n^4 H_n^4 = G_{n+1}/H_{n+1}$. So $\varphi_\alpha^{(n)}(1) = G_n/H_n$ and (3) is proved. ∎

EXAMPLE 1. The degree 512 polynomial G_4 factors in $Z/2[x]$ into irreducible factors of degrees 5, 12, 42, 112, 121, and 220. So any α for which $c(h_\alpha) = 3 + 16^{-4}$ has degree over $Z/2$ equal to one of these integers.

EXAMPLE 2. When α is algebraic the $\varphi_\alpha^{(n)}(1)$ all lie in the finite set $Z/2(\alpha) \cup \infty$. So the function $n \to \varphi_\alpha^{(n)}(1)$ is eventually periodic and $l(\alpha)$ can be easily calculated. For example all α of degree 4 have $l(\alpha) = \infty$, and $c(h_\alpha) = 3$.

REFERENCE

1. P. Monsky, Hilbert–Kunz functions in a family: Point-S_4 quartics, *J. Algebra* **208** (1998), 343–358.